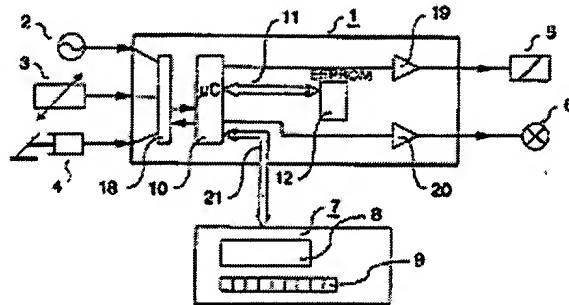


Write protection for EEPROM in electronic control system

Patent number: DE4340027
Publication date: 1995-06-01
Inventor: GLAEBE KLAUS DIPL ING (DE); HOLST HANS DIPL ING (DE); KOESTER HARALD DIPL ING (DE); GUENTHER CONSTANTIN DIPL ING (DE)
Applicant: WABCO VERMOEGENSVERWALTUNG (DE)
Classification:
- **International:** G06F12/14; B60R16/02
- **European:** B60T8/88B, G11C16/10E, G11C16/20, G11C16/22
Application number: DE19934340027 19931124
Priority number(s): DE19934340027 19931124

Abstract of DE4340027

An electronic control system (1) has inputs from a speed sensor (2), temperature sensor (3) and a displacement sensor (4). The inputs are digitised (18) and entered into a microcomputer (10) that receives data from an EEPROM memory (12). An interface (21) connects a diagnostics unit (7) with the microcomputer and outputs are generated to solenoid valves (5) and indicators. The EEPROM has a region of memory defined by the manufacturer as being protected and cannot be accessed. A flag indicates the region. A further region may be selected by the user as being protected.



Data supplied from the **esp@cenet** database - Worldwide

THIS PAGE BLANK (USPTO)

⑯ BUNDESREPUBLIK

DEUTSCHLAND



DEUTSCHES
PATENTAMT

Offenlegungsschrift

⑯ DE 43 40 027 A 1

⑮ Int. Cl. 6:

G 06 F 12/14

// B60R 16/02

⑯ Anmelder:

Wabco Vermögensverwaltungs-GmbH, 30453
Hannover, DE

⑯ Aktenzeichen: P 43 40 027.2
⑯ Anmelddetag: 24. 11. 93
⑯ Offenlegungstag: 1. 6. 95

⑯ Erfinder:

Gläbe, Klaus, Dipl.-Ing., 30161 Hannover, DE;
Günther, Constantin, Dipl.-Ing., 30823 Garbsen, DE;
Holst, Hans, Dipl.-Ing., 30451 Hannover, DE; Köster,
Harald, Dipl.-Ing., 30451 Hannover, DE

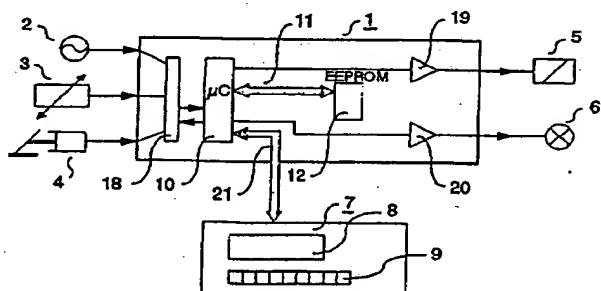
⑯ Für die Beurteilung der Patentfähigkeit
in Betracht zu ziehende Druckschriften:

EP 00 11 136 A1
SU 15 13 459

PETERSEN, Wolfgang: Sicher wie im Safe. In: Elektronikpraxis, Nr. 11, Nov. 1983, S. 8-13;
Elektronik, 24, 1991, S. 140;

⑯ Schreibschutz-Verfahren für einen nichtflüchtigen Schreib-/Lesespeicher in einem elektronischen Steuergerät

⑯ Es wird ein Schreibschutz-Verfahren für einen Speicher (11) eines elektronischen Steuergerätes (1) vorgeschlagen. Dabei wird mindestens ein geschützter Speicherbereich (15) des Speichers (12) festgelegt. Ein Bit des geschützten Speicherbereichs (15) wird zum Schreibschutzflag deklariert. Der Zugriff auf den geschützten Speicherbereich (15) wird vom Zustand dieses Schreibschutzflags abhängig gemacht. Erst unmittelbar vor der Auslieferung des Steuergerätes an den Kunden wird das Schreibschutzflag durch den Hersteller gesetzt.



DE 43 40 027 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 04. 95 508 022/109

7/27

DE 43 40 027 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Schreibschutz-Verfahren für einen nichtflüchtigen Schreib-/Lesespeicher in einem elektronischen Steuergerät gemäß dem Oberbegriff des Patentanspruchs.

Es ist bekannt, elektronische Steuergeräte mit einem Datenspeicher auszurüsten, in welchem verschiedene Datenbereiche definiert sind (DE-PS 41 40 804). Derartige Speicherbereiche können z. B. Fehlermeldungen, Betriebsparameter oder Typbezeichnungen enthalten. Mit einem externen Programmiergerät können in diese Speicherbereiche Daten eingeschrieben oder auch gelöscht werden. Dies kann entweder in der Fabrik während der Herstellung des Gerätes oder später beim Kunden erfolgen.

Bestimmte Speicherbereiche, welche z. B. sensible Daten enthalten, können durch Schutzmaßnahmen gegen einen unbefugten Zugriff geschützt werden. So ist z. B. aus der o. g. Patentschrift bekannt, den Zugriff auf einen Speicherbereich mit Wartungs- oder Reparaturdaten von der Kenntnis eines Passwords abhängig zu machen.

Dasselbe Prinzip wird auch bei den bekannten Bank-Geldautomaten angewendet.

Weiter ist aus der WABCO Bedienungsanleitung für WABCO Diagnose Programmkkarte ABS/ASR "C1"-Generation 446 300 510 2 mit WABCO Diagnostic Controller Set 446 300 321 2, Wabcodruck 815 000 116 3/10.90, Seite 13, bekannt, daß bestimmte Parameter mit einem Schreibschutz versehen sein können. Solche Daten, z. B. Typenbezeichnungen oder Parameter, die auf die Produkthaftung oder auf die Betriebssicherheit des Gerätes Einfluß haben, dürfen von Kunden nicht nachträglich anders eingestellt bzw. überschrieben werden.

Schließlich ist aus der DE-OS 34 10 082 bekannt, bei einem Steuergerät für Kraftfahrzeuge, das mit einem Programmiergerät programmiert werden kann, über eine besondere Freigabe-Leitung eine Hardware-Verriegelung des Speichers gegen unerwünschtes Programmieren zu ermöglichen. Eine derartige Lösung ist jedoch relativ aufwendig.

Der Erfindung liegt die Aufgabe zugrunde, ein wirksames und kostengünstiges Verfahren zur Realisierung eines Schreibschutzes anzugeben.

Diese Aufgabe wird durch das im Patentanspruch angegebene Verfahren gelöst.

Die Erfindung wird im folgenden anhand einer Zeichnung näher erläutert. Dabei zeigt

Fig. 1 das Zusammenwirken eines elektronischen Steuergerätes mit einem Diagnosegerät.

Fig. 2 die Aufteilung eines elektronischen Speichers in verschiedene Datenbereiche.

Fig. 3 ein Flußdiagramm des erfindungsgemäßen Schreibschutz-Verfahrens.

In der Fig. 1 ist mit 1 ein elektronisches Steuergerät bezeichnet, bei dem das erfindungsgemäße Schreibschutz-Verfahren angewendet ist. Dem Steuergerät (1) sind Eingangssignale von einem Drehzahlsensor (2), einem Temperatursensor (3) und einem Wegsensor (4) zugeführt. Die Signale werden in einem Eingangsbaustein (18) digitalisiert und einem Mikrocomputer (10) zugeleitet. Dieser steht über eine Datenverbindung, z. B. einen Bus (11) mit einem Speicher (12), der vorzugsweise als EEPROM (electric eraseable, programmable read only memory) ausgebildet ist, in Verbindung. Der Speicher (12) kann auch Bestandteil des Mikrocomputers (10) sein.

Als Mikrocomputer (10) kann z. B. der Typ AN 8796 BH der Fa. INTEL, und als EEPROM (12) der Typ NMC 93 C 46 der Fa. National Semiconductor verwendet werden.

- 5 An eine Diagnoseschnittstelle (21) des Mikrocomputers (10) ist über Steckverbindungen ein Diagnose- bzw. Programmiergerät (7) mit einer Anzeige (8) und einer Tastatur (9) angeschlossen. Das Gerät (7) kann mit dem Mikrocomputer (10) Daten austauschen. Die Ausgänge des Mikrocomputers (10) sind über Verstärker (19, 20) mit den anzusteuernden Geräten, hier einem Magnetventil (5) und einer Lampe (6), verbunden.

Mit dem Programmiergerät (7) lassen sich auf dem Wege des Datenaustausches mit dem Mikrocomputer (10) in den Speicher (12) Daten einschreiben, aus dem Speicher (12) Daten anzeigen oder auch Daten verändern. Dies kann sowohl beim Hersteller als auch beim Kunden oder in einer Fachwerkstatt erfolgen.

Der Speicher (12) (EEPROM) ist intern in verschiedene Bereiche aufgeteilt (siehe Fig. 2).

In einem Fehlerspeicher (16) kann der Mikrocomputer (10) während seines Betriebes etwa auftretende Fehler nach Art und Ort einspeichern. Diese Funktion dient zur späteren leichteren Fehlersuche und -beseitigung.

Ein weiterer Bereich (15) enthält vom Hersteller eingetragene Typenbezeichnungen und eventuell das Herstellungsdatum der Elektronik.

Ein weiterer Bereich (14) enthält Parameter der Elektronik, die vom Hersteller festgelegt worden sind.

30 Die drei Bereiche (14–16) gelten als Herstellerbereich, die vom Kunden mit Hilfe des Programmiergerätes (7) zwar ausgelesen werden können, deren Daten aber nicht durch den Kunden verändert werden dürfen.

Ein weiterer Bereich (13) des Speichers (12) enthält 35 Kundenparameter. Dieser als Kundenbereich bezeichnete Teil enthält solche Parameter, die von Kunden je nach beabsichtigtem Anwendungsfall abgeändert werden dürfen. Dies können z. B. Grenzgeschwindigkeiten sein, oder bestimmte Anwendungs-Varianten.

40 Zur Verhinderung, daß Unbefugte die Herstellerbereiche (14–16) in unzulässiger Weise überschreiben, sind, wie einleitend beschrieben, Zugangskontrollen (Passwords) bekannt, wodurch nur einem autorisierten Personenkreis der Zugang erlaubt wird.

45 Das in der Fig. 3 dargestellte erfindungsgemäße Schreibschutz-Verfahren verhindert dagegen nach der Auslieferung der Elektronik ein unerwünschtes Überschreiben vollständig. Es wird deshalb vor allem für den Speicherbereich (15) mit den Typennummern und Herstellungsdaten verwendet.

In der Fig. 3 ist ein Abschnitt des Hauptprogramms des Mikrocomputers (10) dargestellt, das mit START beginnt und ENDE endet. Falls ein Außenstehender mit Hilfe seines Programmiergerätes den Speicherbereich (15) auf suchen will, ist dies nur über den Mikrocomputer (10) möglich.

Der Mikrocomputer (10) empfängt vom Programmiergerät (7) über die Diagnoseschnittstelle (21) zunächst eine Aufforderung, Daten in den Speicher (12) einzuschreiben (Block 22).

60 Der Mikrocomputer (10) überprüft daraufhin, ob die gewünschte Speicherstelle innerhalb eines geschützten Bereiches (15) liegt (Block 23). Falls dies der Fall ist, überprüft der Mikrocomputer (10) weiter, ob ein Schreibschutzflag gesetzt ist (Block 24). Falls dies der Fall ist, erfolgt eine Rückmeldung des Mikrocomputers (10) auf seine Diagnoseschnittstelle (21) mit dem Text "Zugriff verweigert" (Block 27). Damit ist ein Zugriff auf

den geschützten Bereich unmöglich.

Das o. g. Schreibschutzflag wird durch den Hersteller des Steuergerätes kurz vor der Auslieferung des Gerätes gesetzt, nachdem die Parametrierung des Bereiches (15) durch den Hersteller erfolgt ist.

Falls der Mikrocomputer (10) feststellt, daß die gewünschte Speicherstelle nicht innerhalb des geschützten Bereiches liegt (Block 23), erlaubt er die Ausführung der Anforderung "Daten in den Speicher (12) schreiben" (Block 25). Als nächstes erfolgt dann eine Rückmeldung auf die Diagnoseschnittstelle (21) mit dem Inhalt "Anforderung ausgeführt" (Block 26).

Da das als Schreibschutzflag definierte Bit selbst im geschützten Speicherbereich liegt, ist ein nachträglicher softwaremäßiger Zugang nicht mehr möglich. Ein Zugriff auf den Speicher (12) ist dann vielmehr nur noch durch einen hardwaremäßigen Eingriff, d. h. (gewaltsames) Öffnen des Elektronik-Gehäuses und Ausbau des Speichers (12), möglich.

Das erfundungsgemäße Verfahren bietet den Vorteil, daß es keine zusätzlichen Kosten durch Hardwaremaßnahmen erfordert, daß während der Fertigung ein uneingeschränkter Zugriff möglich ist, und daß nach Auslieferung an den Kunden ein sicherer Schutz des geschützten Speicherbereiches, der nicht wie z. B. eine Password-Funktion von einem versierten Anwender umgangen werden kann, vorliegt.

Das erfundungsgemäße Verfahren kann nicht nur bei Steuergeräten, sondern auch bei anderen Elektroniken mit Mikrocomputer, wie z. B. Personalcomputern, angewendet werden.

Es ist auch möglich, auch den Kunden-Bereich (13) des Speichers (12) mit einem Schreibschutzflag zu versehen. Dieses kann nach dem Einschreiben oder Ändern von Daten bzw. Parametern durch den Kunden durch diesen gesetzt werden. Dadurch kann der Kunde verhindern, daß unerlaubte weitere Änderungen dieses Bereichs durch Dritte vorgenommen werden.

Patentansprüche

40

1. Schreibschutz-Verfahren für einen nichtflüchtigen Schreib-/Lesespeicher (12) in einem elektronischen Steuergerät (1), wobei der Speicher (12) mit einem Mikrocomputer (10) über eine Datenverbindung, vorzugsweise einen Bus (11) verbunden ist, und wobei der Speicher (12) verschiedene Bereiche aufweist, u. a. Bereiche für typ- und/oder kunden-spezifische Daten wie Typenbezeichnungen und Parameter, gekennzeichnet durch folgende Merkmale:

- a) es wird mindestens ein geschützter Speicherbereich (15) festgelegt,
- b) ein Bit des geschützten Speicherbereichs (15) wird zum Schreibschutzflag deklariert;
- c) der Zugriff auf den geschützten Speicherbereich (15) wird vom Zustand des Schreibschutzflags abhängig gemacht;
- d) erst nach der Eingabe der zu schützenden Daten in den geschützten Speicherbereich (15) durch den Hersteller wird das Schreibschutzflag gesetzt.

2. Schreibschutz-Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß auch der Kunden-Bereich (13) des Speichers (12) mindestens einen geschützten Bereich enthält, dessen Schreibschutzflag nach dem Einschreiben oder Ändern von Daten durch den Kunden gesetzt werden kann.

3. Einrichtung zur Durchführung des Verfahrens nach Anspruch 1, mit folgenden Merkmalen:

- a) es ist ein elektronisches Steuergerät (1) mit einem Mikrocomputer (10) und einem Speicher (12) vorgesehen,
- b) es ist ein Programmiergerät (7) vorgesehen,
- c) das Steuergerät (1) ist mit dem Programmiergerät (7) über einen Bus (21) verbindbar,
- d) der Mikrocomputer (10) ist mit dem Speicher (12) über eine Datenverbindung, vorzugsweise einen weiteren Bus (11) verbunden,
- e) der Speicher (12) ist so ausgebildet, daß er mindestens einen durch einen Schreibschutzflag geschützten Bereich (15) aufweist, wobei das Schreibschutzflag durch den Hersteller oder den Kunden setzbar ist.

Hierzu 3 Seite(n) Zeichnungen

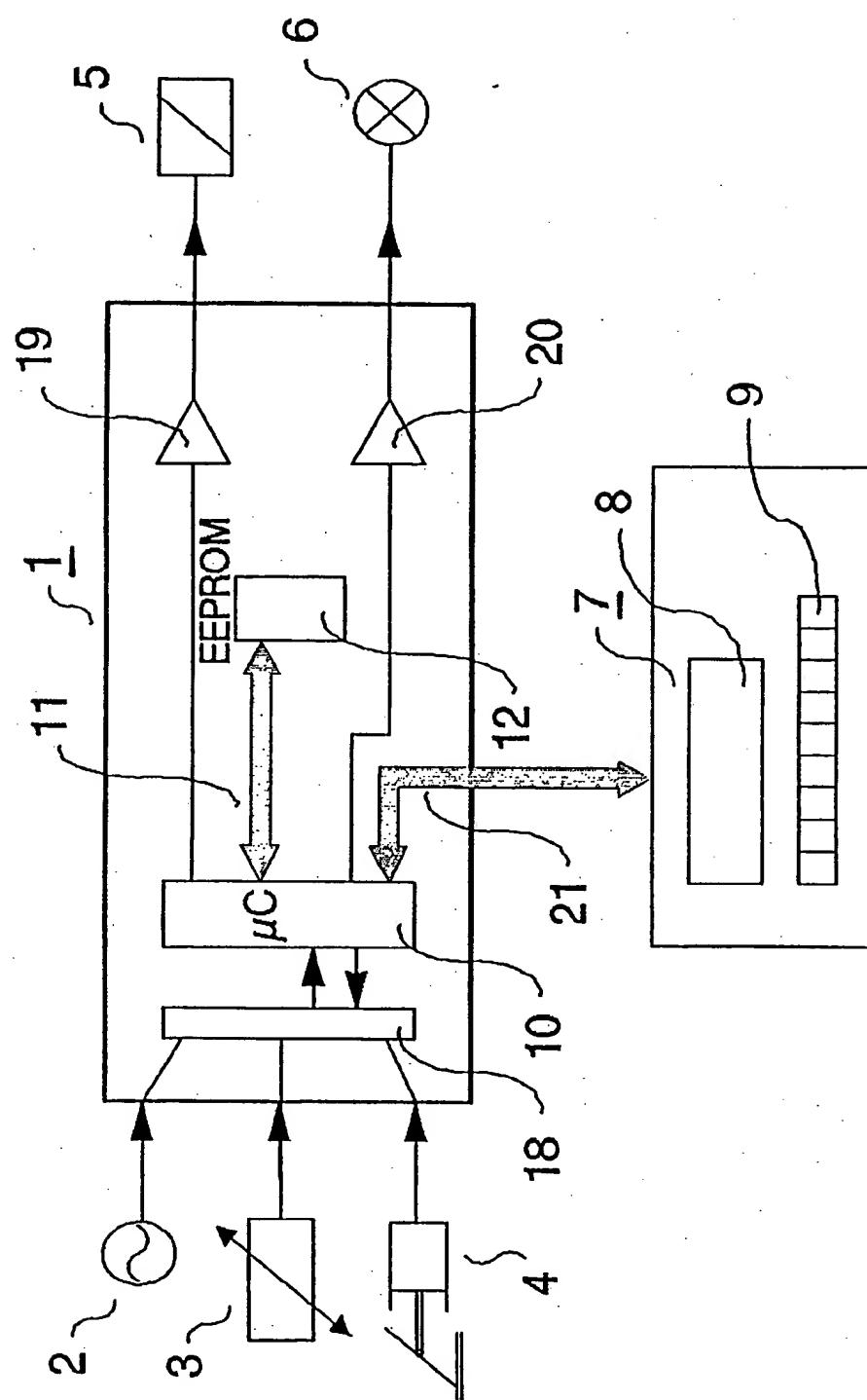


FIG.1

EEPROM

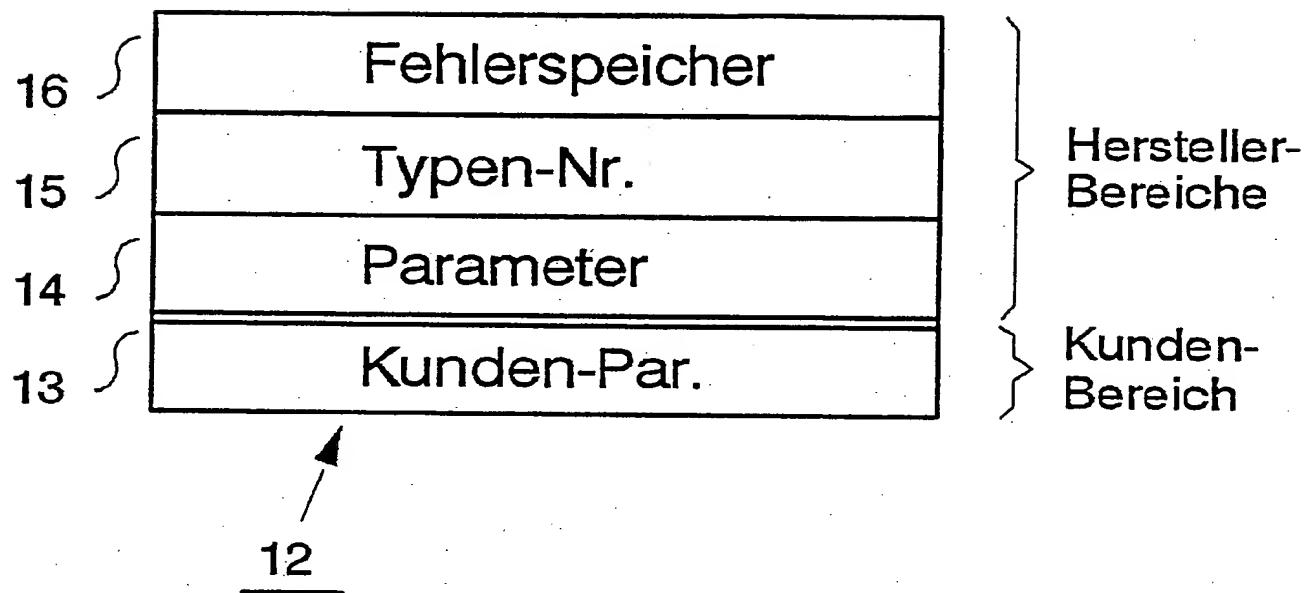


Fig.2

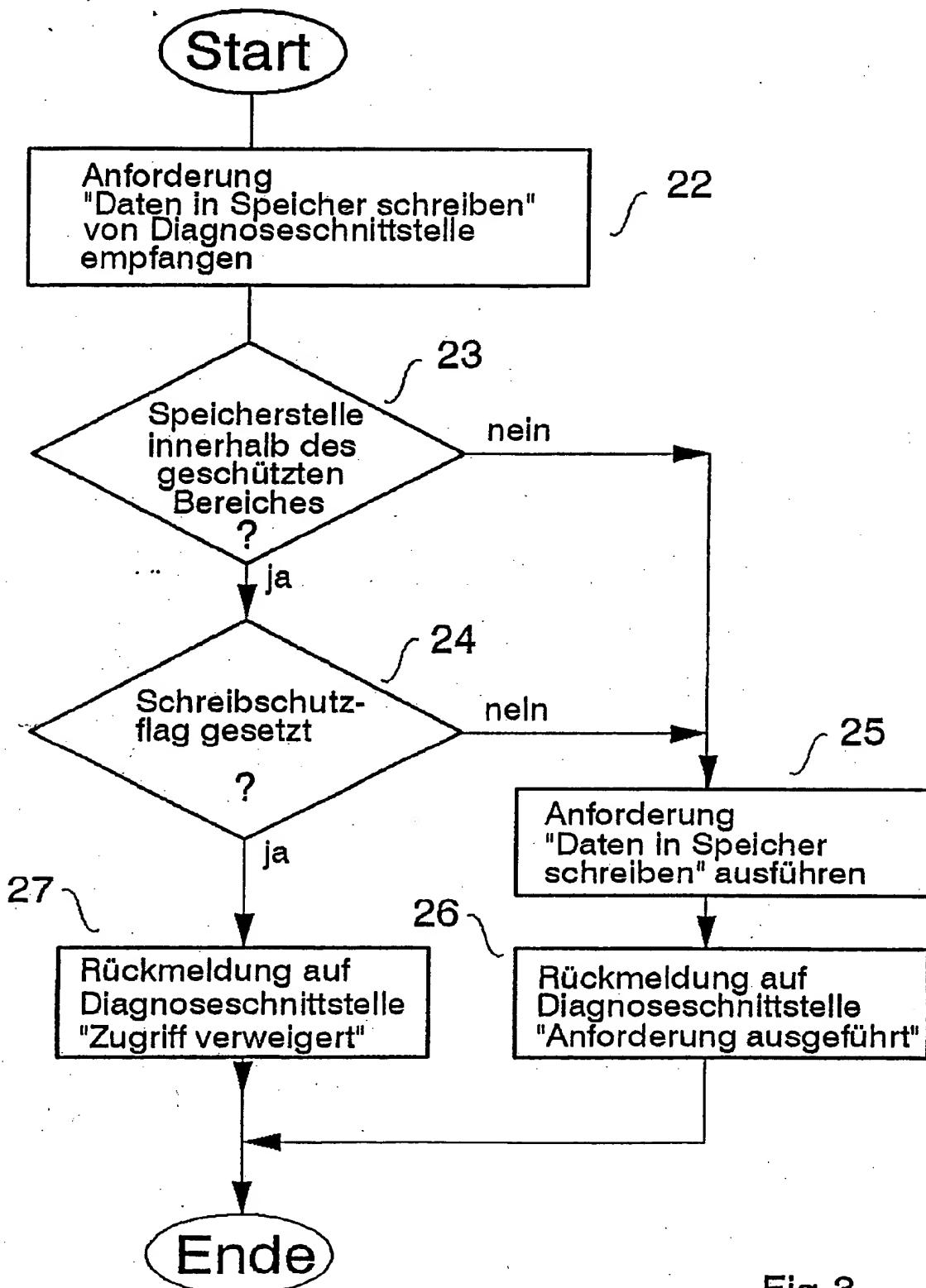


Fig.3